Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

On a Certain Group of Isomorphisms.

By John Wesley Young.

Let G denote the non-abelian group of order p^m (p an odd prime) which contains operators of order p^{m-1}. It is the object of the present paper to discuss the properties and ultimately (§7) to determine the defining relations of the group of isomorphisms of G. The writer wishes to express his indebtedness to Professor G. A. Miller for helpful suggestions offered during its preparation.

§1.—*Combinatory Laws and Subgroups of G.*

The defining relations of G are*

$$P^{p^{m-1}}=1, \quad Q^p=1, \quad Q^{-1}PQ=P^{1+p^{m-2}}.$$

If we denote any operator $P^\alpha Q^\beta$ of G by $[\alpha, \beta]$, the product of any two operators $[\alpha, \beta]$ and $[\gamma, \delta]$ is given by

$$[\alpha, \beta][\gamma, \delta]=[\alpha+\gamma-\beta\gamma p^{m-2}, \quad \beta+\delta]; \tag{I}$$

by repetition we obtain

$$[\alpha, \beta]^n=[n\alpha-\tfrac{1}{2}n(n-1)\alpha\beta p^{m-2}, \quad n\beta]. \tag{II}$$

In these formulæ, the first number in the brackets is to be taken mod p^{m-1}, the second mod p.

All the subgroups in G are abelian. Moreover, G contains just $p+1$ subgroups of every order p^s, of which p are cyclic (generated by $[p^{m-s-1}, x]$, $x=0, 1, 2, \ldots, p-1$) and one is abelian of type $(s-1, 1)$, except when

---

* Burnside, "Theory of Groups of Finite Order" (1897), p. 76.

$s = 1$.[*] Since, by (II), we have $[\alpha, \beta]^p = [\alpha p, 0]$, the cyclic subgroup of order p^s, generated by $[p^{m-s-1}, 0]$ $(s < m-1)$, is contained in all the subgroups of order p^{s+1}; it is therefore characteristic. The non-cyclic subgroups are evidently characteristic. Hence, *G contains a characteristic cyclic subgroup of every order p^s, when $1 \leqq s < m-1$; and a characteristic non-cyclic subgroup of everg order $p^{s'}$, when $1 < s' < m$.*

§2.—*Defining Correspondence of any Holomorphism of G.*

Let the correspondence

$$\begin{aligned} P &\sim P^{\alpha} Q^{\beta}, \\ Q &\sim P^{\gamma p^{m-2}} Q^{\delta}, \end{aligned} \qquad [\alpha \not\equiv 0 \bmod p,\ \beta,\ \gamma,\ \delta < p],$$

define an holomorphism[†] of G. Applying (I), (II) of §1, this assumption leads at once to the correspondence

$$[a, b] \sim [a\alpha + (b\gamma - \tfrac{1}{2} a(a-1)\alpha\beta)p^{m-2},\ a\beta + b\delta],$$

where $[a, b]$ is any operator of G. The product of the operators corresponding to any two, $[a, b]$ and $[c, d]$, must be the operator corresponding to $[a, b][c, d] = [a + c - bcp^{m-2}, b + d]$ for all values of a, b, c, d. Calculating the expressions and equating the coefficients of a, b, c, d, we find the necessary and sufficient condition for this equality to be

$$\delta \equiv 1 \bmod p.$$

Moreover, it is readily shown that the assumption leads to a one-to-one correspondence. Hence, *the correspondence*

$$C = \left\{ \begin{aligned} P &\sim P^{\alpha} Q^{\beta}\ , \\ Q &\sim P^{\gamma p^{m-2}} Q, \end{aligned} \right\} \qquad [\alpha \not\equiv 0 \bmod p,\ \beta < p,\ \gamma < p$$

defines an holomorphism for any set α, β, γ; and every holomorphism of G is given by C.

Hence, since α may take $p^{m-2}(p-1)$ non-congruent values mod p^{m-1} and β, γ each p non-congruent values mod p, *the order of the group of isomorphism I of G is $p^m(p-1)$.*

---

[*] Burnside, loc. cit., p. 76.

[†] The word "holomorphism" is used in place of "holoedric isomorphism."

§3.—*Analytic Expression for any Operator in I.—Numbers α, β, γ giving rise to a Subgroup of I.*

Regarding I as a substitution group on the p^m operators of G, any operator S_i of I is completely represented by the expression

$$S_i = \mid [a\alpha_i + (b\gamma_i - \tfrac{1}{2}a(a-1)\alpha_i\beta_i)\,p^{m-2},\ a\beta_i + b] \mid,$$

where the notation

$$S = \mid [M, N] \mid$$

signifies that S replaces $[a, b]$ by $[M, N]$. For every set $(\alpha_i, \beta_i, \gamma_i)$, S_i represents an operator of I. For a properly chosen system of sets, S_i may be made to represent the operators of any subgroup of I.

Let S_1 in $(\alpha_1, \beta_1, \gamma_1)$ and S_2 in $(\alpha_2, \beta_2, \gamma_2)$ be any two operators of I. Then, if $S_1 S_2$ is an operator of the same kind in $(\alpha_3, \beta_3, \gamma_3)$, by calculating the expression for $S_1 S_2$ in terms of $(\alpha_1, \beta_1, \gamma_1, \alpha_2, \beta_2, \gamma_2)$ and equating coefficients of a and b, we find

$$2\alpha_3 + \alpha_3\beta_3 p^{m-2} \equiv 2\alpha_1\alpha_2 + (2\beta_1\gamma_2 + \alpha_1\alpha_2(\beta_1 + \beta_2))\,p^{m-2} \mod p^{m-1}. \qquad (A_1)$$

$$\beta_3 \equiv \beta_1 + \alpha_1\beta_2 \mod p, \qquad (A_2)$$

$$\gamma_3 \equiv \gamma_2 + \alpha_2\gamma_1 \mod p. \qquad (A_3)$$

In order that a system of sets $(\alpha_i, \beta_i, \gamma_i)$ may represent a subgroup of I, it is necessary and sufficient that, if from the system any two sets $(\alpha_1, \beta_1, \gamma_1)$ and $(\alpha_2, \beta_2, \gamma_2)$ be selected, the set $(\alpha_3, \beta_3, \gamma_3)$ defined by (A_1), (A_2), (A_3) be in the system.

§4.—*Invariant Subgroups of Order p^3 and p^2 in I.*

The correspondence C (§2) shows that the characteristic cyclic subgroup of order p^{m-2} (§1) may correspond to itself in $p^{m-3}(p-1)$ ways; i. e., I contains as a constituent the group of isomorphisms of this cyclic group. The group of isomorphisms of a cyclic group of order p^{m-2} being cyclic, *I contains as a constituent the cyclic group of order $p^{m-3}(p-1)$, and hence an invariant subgroup of order p^3.* Let the latter be denoted by H_3. Since H_3 leaves $\{P^p\}$ unchanged, the operators of H_3 are obtained from the general operator S_i (§3) by restricting α_i to values congruent to unity mod p^{m-2}. Putting $\alpha_i = 1 + \alpha_i' p^{m-2}$, any operator of H_3 is represented by

$${}_3S_i = \mid [a + (a\alpha_i' + b\gamma_i - \tfrac{1}{2}a(a-1)\beta_i)\,p^{m-2},\ \ a\beta_i + b] \mid,$$
$$[\alpha_i' < p,\ \ \beta_i < p,\ \ \gamma_i < p].$$

(It may be noted that the system of sets $(\alpha_i', \beta_i, \gamma_i)$ satisfies the conditions of §3.)

Placing the coefficient of p^{m-2} in ${}_3S_i$ equal to A_i, we way write the n^{th} power of ${}_3S_i$ as follows:

$$ {}_3S_i^n = |\,[a + (nA_i + \tfrac{1}{2}n(n-1)\,a\beta_i\gamma_i)\,p^{m-2},\ na\beta_i + b]\,|. $$

Hence $$ {}_3S_i^p = |\,[a, b]\,| = 1; $$

i. e., all the operators of H_3 (except identity) are of order p. Moreover H_3 is non-abelian. For we have

$$ {}_3S_i \cdot {}_3S_j = |\,[a + (A_i + A_j + a\beta_i\gamma_j)\,p^{m-2},\ a(\beta_i + \beta_j) + b]\,|, $$

which shows that ${}_3S_i$ and ${}_3S_j$ are not in general commutative. Hence, H_3 *is the non-abelian group of order* p^3, *all of whose operators (except identity) are of order* p.*

Hence also I *is non-abelian.*

The characteristic non-cyclic subgroup of order p^{m-1} is made by C to correspond to itself in $p^{m-2}(p-1)$ ways; I therefore contains an invariant subgroup H_2 of order p^2; H_2 being contained in H_3 is abelian of type (1, 1),

§5.—*Invariant Subgroup H_m of Order p^m in I.*

By Sylow's theorem, I contains a single subgroup of order p^m; let it be denoted by H_m. To obtain a general operator ${}_mS_i$ of H_m, we must find a suitable system of sets $(\alpha_i, \beta_i, \gamma_i)$ satisfying (A_1), (A_2), (A_3) of §3.

Restrict α_i to the p^{m-2} values which are congruent to unity mod p; (A_1), (A_2), (A_3) are then equivalent to

$$ \begin{aligned} \alpha_3 &\equiv \alpha_1\alpha_2 + \beta_1\gamma_2\,p^{m-2} \mod p^{m-1}, \\ \beta_3 &\equiv \beta_1 + \beta_2 \mod p, \\ \gamma_3 &\equiv \gamma_1 + \gamma_2 \mod p. \end{aligned} $$

Evidently $(\alpha_3, \beta_3, \gamma_3)$ is in the system for any choice of $(\alpha_1, \beta_1, \gamma_1)$ and $(\alpha_2, \beta_2, \gamma_2)$. Hence the system gives rise to a subgroup of I; this subgroup is of order p^m, and hence is H_m We have then

---

* Burnside, loc. cit., p. 82.

$$ {}_mS_i = |[a\alpha_i'' + (b\gamma_i - \tfrac{1}{2}a(a-1)\beta_i)p^{m-2},\ a\beta_i + b]|, $$
$$ [\alpha_i'' \equiv 1 \bmod p,\ \beta_i < p,\ \gamma_i < p. $$

If $\beta_i = \gamma_i = 0$, the resulting p^{m-2} operators are invariant in H_m, as is readily shown by forming the product ${}_mS_j'\,{}_mS_i$, where ${}_mS_j' = |[a\alpha_j'', b]|$. Moreover, H_m contains an invariant operator of order p^{m-2}. For we have

$$ {}_mS_j'^n = |[a\alpha_j''^n, b]| $$

and if $\alpha_j'' = 1 + kp\ (k < p)$, p^{m-2} is the smallest value of n which will satisfy $\alpha_j''^n \equiv 1 \bmod p^{m-1}$.

Further, H_m contains no operator of order p^{m-1}. For, we find

$$ {}_mS_i^n = |[a\alpha_i''^n + (nb\gamma_i - \tfrac{1}{2}na(a-1)\beta_i + \tfrac{1}{2}n(n-1)a\beta_i\gamma_i)p^{m-2},\ na\beta_i + b]| $$

and if $n = p^{m-2}$, ${}_mS_i^n = 1$ for every set $(\alpha_i'', \beta_i, \gamma_i)$.

Hence, H_m *is the non-abelian group of order* p^m *which contains an invariant operator of order* p^{m-2}, *and does not contain any operator of order* p^{m-1}. Its defining relations are :*

$$ I_1^{p^{m-2}} = 1,\quad J^p = 1,\quad K^p = 1,\quad K^{-1}JK = JI_1^{p^{m-3}},\quad I_1J = JI_1,\quad I_1K = KI_1. $$

It may be noted that ${}_mS_j'$ makes every operator of G correspond to its α_j''th power. In a previous paper† it has been shown that all such holomorphisms are invariant in the group of isomorphisms; i. e., the operators ${}_mS_j'$ are invariant in I, which also follows readily analytically. By another theorem in the same paper, it follows at once that they form a cyclic subgroup H_{m-2} of order p^{m-2} in I; this agrees with the result already obtained.

§6.—*The Quotient-Group* I/H_{m-2}.

H_{m-2} leaves all the subgroups of G fixed. Regarding I/H_{m-2} of order $p^2(p-1)$ as a substitution group on the subgroups of G, it is clear that I/H_{m-2} must contain a transitive constituent T_1 of degree p on the p cyclic subgroups of order p_{m-1}. T_1 is doubly transitive; for the correspondence

$$ P \sim P^a,\quad Q \sim Q $$

---

* Burnside, loc. cit., p. 78.

† Transactions of the American Mathematical Society, Vol. III (1902), p. 189.

leaves $\{P\}$ fixed, while it transforms any of the other cyclic subgroups of order p^{m-1}, $\{PQ\}$, into $\{P^{\alpha}Q\}$. Non-congruent values of α mod p give different subgroups; by assigning to α any of its $p-1$ non-congruent values mod p, $\{PQ\}$ may be transformed into any one of the remaining $p-1$ subgroups. The order of T_1 cannot be $p^2(p-1)$, since the order must be a divisor of $p\,!$; it must then be $p(p-1)$, since there is no doubly transitive group of degree p and order less than $p(p-1)$. Hence T_1 is a metacyclic group of degree p.

Further, I/H_{m-2} must contain a transitive constituent T_2 of degree p on the p non-characteristic subgroups of G of order p. Reasoning similar to the above shows that T_2 also is a metacyclic group of degree p. Moreover, it is possible to leave the subgroups of order p^{m-1} fixed, and still permute the subgroups of order p according to a group of order p. Hence, I/H_{m-2} *is obtained by establishing a* (p, p)*-isomorphism between two metacyclic groups of degree* p.

§7.—*The Defining Relations of I.*

If we take

$$I_1 = |[a + ap, b]|, \quad J = |[a + bp^{m-2}, b]|,$$
$$K = |[a + \tfrac{1}{2}a(a-1)p^{m-2}, \quad -a + b]|,$$

then I, J, K satisfy the relations defining H_m (§5). For, we have

$$K^{-1}JK = |[a + (a+b)p^{m-2}, b]| = JI_1^{p^{m-3}}$$

and the other five relations may easily be verified.

Corresponding to every operator of order $p-1$ in I/H_{m-2}, there is in I just one operator of order $p-1$. Let

$$I_2 = |[a\alpha, b]|$$

be one of these, where α belongs to exponent $p-1$ mod p^{m-1}. Then, we have

$$I_2^{-1}JI_2 = |[a + \alpha bp^{m-2}, b]| = J^{\alpha}.$$

Also $I_2^{-1}KI_2$ replaces $[a\alpha, b]$ by $[a\alpha + \frac{1}{2}a(a-1)\alpha p^{m-2}, \ -a + b]$. This is effected by an operator

$$S_3' = |[a + (a\alpha_3' + \tfrac{1}{2}a(a-1)\beta_3)p^{m-2}, \ -a\beta_3 + b]|,$$

α_3', β_3 being defined by the relations

$$\alpha\beta_3 - 1 \equiv 0, \quad 2\alpha\alpha_3 + \alpha - 1 \equiv 0 \quad \text{mod } p.$$

We find readily

$$S_3' = K^{\beta_3} \big| [a + a\alpha_3' p^{m-2}, b] \big| = K^{\beta_3} I_1^{\alpha_3' p^{m-3}}.$$

Placing $I_1 I_2 = I_3$, since I_1 is commutative with I_2, J, K, we may *write the defining relations of I as follows*:

$$I^{p^{m-2}(p-1)} = 1, \quad J^p = 1, \quad K^p = 1, \quad I_3^{-1} J I_3 = J^x, \quad I_3^{p-1} K = K I_3^{p-1},$$

$$I_3^{-1} K I_3 = K^s I_3^{t p^{m-3}(p-1)}, \quad K^{-1} J K = J I_3^{p^{m-3}(p-1)}$$

where x is any number belonging to exponent $p-1$ mod p^{m-1}, and where s, t are defined by the relations

$$\left.\begin{aligned} sx - 1 &\equiv 0, \\ 2xt + x - 1 &\equiv 0 \end{aligned}\right\} \mod p.$$

CORNELL UNIVERSITY.